الأمن السيبراني والشمول المالي في ظل التحول الرقمي للقطاع المالي (التهديدات السيبرانية، اليات التحوط)

Cybersecurity and financial inclusion in the context of the digital transformation of the financial sector (threatsecurity and hedging mechanisms)

جميلة جغل[1]*، عادل زقرير[2]

[1] مخبر النمو والتنمية الاقتصادية في الدول العربية, جامعة الشهيد حمه لخضر –الوادي– (الجزائر), djeghel-djamila@univ-eloued.dz

[2] جامعة الشهيد حمّه لخضر الوادي (الجزائر)، Zegrier-adel@univ-eloued.dz

تاريخ الاستلام: 2023/05/01؛ **تاريخ المراجعة**: 2023/05/05؛ **تاريخ النشر**: 2023/06/30

ملخص: هدف هذه الدراسة إلى تسليط الضوء على أهمية الأمن السيبراني ضمن إستراتيجية التحول الرقمي للقطاع المالي لتوسيع نطاق الشمول المالي، حيت أدى تزايد الاعتماد على الخدمات المالية الرقمية وخصوصا في القطاعات المالية للدول النامية إلى تزايد التهديدات السيبرانية عليها، لان مجرمو الإنترنيت لاحظوا ذلك ووجدوا فيها غاياتهم نظرا لضعف تدابير الأمن السيبراني في هذه الدول.

وتوصلت الدراسة إلى أن التحول الرقمي للقطاع المالي حقق انجازا كبيرا في زيادة معدلات الشمول المالي, ولكن في نفس الوقت جلب مخاطر سيبرانية تفوق حجم الكوارث الطبيعية وأصبحت تهدد الاستقرار المالي والنظام المالي بأكمله, مما أوجب التركيز والاهتمام بالأمن السيبراني في سياق الشمول المالي أكثر من أي وقت مضى, وذلك بإتباع آليات التحوط التي وضعتها الجهات المختصة لحماية النظام المالي ومكاسب الشمول المالي التي حققها التحول الرقمي من التهديدات السيبرانية, ولضمان الاستمرارية في مواصلة جهود الشمول في تحقيق أهداف التنمية المستدامة.

الكلمات المفتاحية:الأمن السيبراني، التحول الرقمي، القطاع المالي، الشمول المالي، الخدمات المالية الرقمية، التهديدات السيبرانية.

تصنيف JEL :G21؛ G28؛ G38؛ K42؛ L86؛ O33؛ O38

Abstract: The aim of this study is to highlight the importance of cybersecurity in the digital transformation strategy of the financial sector, in order to expand financial inclusion. The increased reliance on digital financial services, especially in developing countries, has led to an increase in cyber threats, as cybercriminals have found opportunities due to weak cybersecurity measures in these countries.

The study found that the digital transformation of the financial sector has achieved significant success in increasing financial inclusion rates, but at the same time, it has brought cyber risks that surpass the size of natural disasters and threaten financial stability and the entire financial system. This has made it necessary to focus on cybersecurity in the context of financial inclusion more than ever before, by following the hedging mechanisms developed by relevant authorities to protect the financial system and the financial inclusion gains achieved through digital transformation from cyber threats, and to ensure the continuity of efforts to achieve sustainable development goals.

Keywords:cybersecurity, digital transformation, financial sector, financial inclusion, digital financial services, cyber threats.

Jel Classification Codes : G21;G28;G38; K42;L86;O33;O38.

I- تمهيد :

يعد الشمول المالي هدفا إستراتيجيا لأغلب دول العالم، منذ أن أقرت مجموعة العشرين بالشمول المالي كأحد ركائز أجندة التنمية العالمية في 2010، وتعهدت بتعزيزه في كافة أنحاء العالم، وأعادت تعهدها بدمج الخدمات المالية الرقمية في 2016، وفي هذا السياق،يشهد القطاع المالي للدول النامية تسارعا غير مسبوق نحو التوجه إلى التحول الرقمي بالاعتماد على أدوات التكنولوجيا المالية لتوسيع نطاق الشمول المالي، إلا أن مجرمو الانترنيت استغلوا هذا التحول ووجدوا طرقا جديدة لمهاجمة البيانات وخرقها في البنوك، ومع التزايد الكبير في حجم وتعقيدات الهجمات السيبرانية، أصبح الأمن السيبراني مصدر قلق كبير في كافة أنحاء العالم، وهذا ما جعل هذه المسألة مطروحة بشدة على أجندة اجتماعات الجهات الرقابية والإشرافية والمؤسسات المالية.

- **إشكالية الدراسة:**

وعلى ضوء ما تقدم نحاول في هذه الورقة البحثية الإجابة على التساؤل التالي:

" ما مدى أهمية الأمن السيبراني ضمن إستراتيجية التحول الرقمي للقطاع المالي لتوسيع نطاق الشمول المالي؟"

ويندرج عن التساؤل الرئيسي التساؤلات الفرعية التالية:

- كيف يساهم التحول الرقمي للقطاع المالي في دعم الشمول المالي؟
- لماذا تزايدت التهديدات السيبرانية على القطاع المالي ؟
- كيف يمكن التحوط من تهديدات الأمن السيبراني على القطاع المالي؟

- **فرضيات الدراسة:**

من أجل الإجابة على التساؤلات الفرعية السابقة قمنا بصياغة الفرضيات الآتية:

- يسرع التحول الرقمي للقطاع المالي وبالاعتماد على التكنولوجيا المالية نفاذ الخدمات المالية الرقمية، ووصولها إلى أكبر شرائح ممكنة من المجتمع، مما يزيد من فرص توسيع الشمول المالي.
- تزايدت التهديدات السيبرانية على القطاع المالي نظرا لدوره الحيوي في الوساطة المالية، ومع التزايد الكبير في اعتماده على الخدمات المالية الرقمية ضمن إستراتيجية توسيع نطاق الشمول المالي، مما جعله هدفا جذابا لمجرمو الانترنيت.
- بإتباع آليات التحوط التي وضعتها المؤسسات المالية الدولية والهيئات الرقابية والإشرافية والتي تنص على توحيد الجهود الدولية والتدريب على المرونة السيبرانية وتنمية القدرات, والإقتداء بتجارب الدول الناجحة في هذا المجال.

- **أهمية وأهداف الدراسة:**

تستمد هذه الدراسة أهميتها من موضوعها في حد ذاته، حيث تصاعد الاهتمام العالمي بالأمن السيبراني في سياق الشمول المالي، وخصوصا بعد تزايد التهديدات السيبرانية على منصات الخدمات المالية الرقمية، وذلك لمحاولة البحث عن حلول للحد من هذه التهديدات، وتسليط الضوء على تخصص الأمن السيبراني الذي أصبح مطلوبا في جميع المجالات،كما أنها تعتبر من المواضيع الحديثة والنادرة في المراجع العلمية والأبحاث الأكاديمية، وتهدف هذه الورقة البحثية إلى تحديد مفهوم كل من الشمول المالي والأمن السيبراني، وعرض أهم مؤشرات مكاسب الشمول المالي التي حققها التحول الرقمي وبعض إحصائيات التهديدات السيبرانية على القطاع المالي، وفي الأخير التركيز على آليات التحوط من تهديدات الأمن السيبراني على القطاع المالي لحماية مكاسب الشمول المالي التي حققها التحول الرقمي.

- **منهجية الدراسة:**

سنعتمد في هذه الدراسة على الأسلوب الوصفي التحليلي وذلك بوصف المفاهيم الخاصة بهذه الدراسة، أما التحليلي من خلال تحليل مجموعة من المؤشرات والبيانات التي تخدم الدراسة.

- **هيكل الدراسة:**

لتحقيق أهداف الدراسة قمنا بتقسيم هذه الورقة البحثية إلى جزئين، جزء نظري ونتناول فيه الإطار المفاهيمي لكل من الشمول المالي والأمن السيبراني، وجزء تطبيقي نقوم فيه بعرض وتحليل مؤشرات مكاسب الشمول المالي التي حققها التحول الرقمي وبيانات تهديدات الأمن السيبراني على القطاع المالي و آليات التحوط منها .

الإطار النظري للدراسة

أولا: الشمول المالي

يحظى موضوع تعزيز الوصول إلى التمويل والخدمات المالية وخصوصا في الدول النامية، باهتمام كبير من قبل مجلس محافظي البنوك المركزية والمؤسسات المالية الدولية، إدراك منهم للفرص الكامنة والكبيرة التي يمكن تحقيقها من خلال تعزيز الشمول المالي لدعم التنمية المستدامة ومواجهة تحديات البطالة وتحقيق العدالة والتقليل من حدة الفقر (العربي، 2021).

1- تعريف الشمول المالي:

"الشمول المالي أو الاشتمال المالي، مصطلح أطلق عليه العديد من التعريفات، ولعل أبرزها: إدخال أو دمج الفئات التي يطلق عليها مهمشة ماليا أو من ذوي الدخل المالي المنخفض الذي لا يسمح لها بالانخراط في عمليات النظام المصرفي، بالتعامل مع الجهاز المصرفي من خلال منظومة العمل الرقمية، بمعنى إتمام جميع التعاملات المالية بطريقة إلكترونية، ويهتم الشمول المالي بتقديم الخدمات المالية باستخدام الطرق السهلة والبسيطة وبأقل التكاليف، مثل الدفع عن طريق الهاتف المحمول" (لوزري، 2021، صفحة 15).

كما عرفته كل من مجموعة العشرين(G20) ومؤسسة التحالف العالمي للشمول المالي (AFI) بأنه"تعزيز وصول واستخدام كافة فئات المجتمع، وبما يشمل الفئات المهشمة والميسورة للخدمات والمنتجات المالية، التي تتناسب مع احتياجاتهم،ب حيث تقدم لهم بشكل عادل وشفاف وبتكاليف معقولة" (صندوق النقد العربي، 2015).

وعرفه **البنك الدولي** بأنه "يعني أن الأفراد والشركات يستطيعون الحصول على منتجات مالية مفيدة وبأسعار معقولة تلبي احتياجاتهم من المعاملات والمدفوعات والادخار والائتمان والتامين،التي يتم تقديمها بطريقة مسؤولة ومستدامة" (Abdelfateh, 2018)

ويشير **الشمول المالي الرقمي** وهو الأقرب لدراستنا، إلى القدرة على الوصول من خلال التكنولوجيا الرقمية للخدمات المالية الرسمية واستخدامها من قبل السكان غير المشمولين ماليا، بحيث تكون هذه الخدمات مناسبة لاحتياجات العملاء، ويتم تقديمها بطريقة مسؤولة ومستدامة وبتكلفة مقبولة ضمن إطار تشريعي وقانوني ملائم، ويجب كذلك أن تمثل تلك الخدمات المالية الرقمية للمتطلبات التنظيمية المعمول بها، على مكافحة غسل الأموال، وتمويل الإرهاب وحماية المستهلك والأمن السيبراني، وحماية الخصوصية. (حسن، 2022، صفحة 2251)

2- مبادئ مجموعة العشرين (G20)عالية المستوى بدمج الخدمات المالية الرقمية في تعزيز الشمول المالي:

تبنت دول مجموعة العشرين في عام 2016، مباديء إرشادية للتمويل الرقمي تنطرق إلى الإجراءات الواجب العمل عليها لتسريع رقمنة الشمول المالي (الشمول المالي الرقمي)، تؤكد الحاجة إلى إستخدام التقنيات الرقمية لتوفير منتجات مالية ذات جودة عالية ومناسبة للسكان المستبعدين ماليا. وإستكمالا لمساعيها في هذا الإطار، أصدرت الشراكة العالمية لمجموعة العشرين تحت رئاسة المملكة السعودية في

عام 2020 المباديء التوجيهية رفيعة المستوى بشأن سياسات الشمول المالي الرقمي للشباب والنساء والشركات الصغيرة والمتوسطة تتوزع المبادىء الثمانية على أربع مجموعات رئيسية كالآتي (طلحة و صبري، 2020):

أ- ضمان بنية تحتية مالية رقمية مرنة ومسؤولة

- **المبدأ الأول:** دعم تطوير بنية تحتية رقمية آمنة ومسؤولة، يسهل الوصول إليها على نطاق واسع ونظام دفع قابل للتشغيل البيني، وضمان تنافسية المؤسسات المالية.
- **المبدأ الثاني:** تشجيع توفير المنتجات المالية الرقمية الملائمة للاحتياجات وذات الكلفة المقبولة مع ضمان تقديم هذه الخدمات بما يتماشى مع المتطلبات الدولية لمكافحة غسل الأموال وتمويل الإرهاب، وإجراءات العناية الواجبة للعملاء ونظام الهوية الرقمية.

ب - تعزيز صنع السياسات المسؤولة والشاملة

- **المبدأ الثالث:** تحسين توافر ودقة البيانات فيما يتعلق بالنفاذ إلى المنتجات والخدمات المالية الرقمية واستخداماتها.
- **المبدأ الرابع:** دعم تبني السياسات والمبادرات التي تستهدف زيادة الشمول المالي الرقمي في الاستراتيجيات الوطنية.

ج- تعزيز النمو الشامل من خلال إطار تنظيمي ممكن للخدمات المالية الرقمية

- **المبدأ الخامس:** دعم الإصلاحات التنظيمية والقانونية التي تحد من عدم المساواة في الوصول إلى الخدمات المالية الرقمية، التي ينتج عنها عدم المساواة الاجتماعية والاقتصادية.
- **المبدأ السادس:** النظر في تطوير إطار تنظيمي يدعم الابتكار الرقمي في القطاعين العام والخاص.

د- تعزيز المعرفة الرقمية والمالية وبناء القدرات ودعم المتعاملين وحماية البيانات ضد المخاطر المحتملة

- **المبدأ السابع:** تعزيز الثقافة المالية والتجارية والرقمية وبناء القدرات من خلال التدخلات التي تستهدف دعم الشمول المالي الرقمي بالاستفادة من انتشار التقنيات.
- **المبدأ الثامن:** دعم إجراءات حماية العملاء المالية، بما في ذلك حماية البيانات، بما يلبي احتياجات الشباب والنساء والشركات الصغيرة والمتوسطة.

3- أبعاد ومؤشرات الشمول المالي:

يتضمن الشمول المالي عدة أبعاد أهمها (استخدام الخدمات المالية، الوصول للخدمات المالية، جودة الخدمات المالية)، وكل واحدة من هذه الأبعاد لها آثار على العلاقة بين مقدمي الخدمات المالية وعملائهم، ولكل منها دور مختلف في تحقيق الشمول المالي، وقد استخدمت مجموعة من هذه الأبعاد الثلاثة في مختلف الجهود المبذولة لجمع البيانات المتعلقة بالشمول المالي من قبل صندوق النقد الدولي ومؤسسة التحالف العالمي للشمول المالي والبنك الدولي. ولقياس مستويات الشمول المالي وتطوره في مختلف البلدان، وإجراء المقارنات الدولية، أطلقت مجموعة البنك الدولي عدة مؤشرات، نوضح مفهوم أبعاد الشمول المالي ومؤشراته في الجدول الآتي:

الجدول (1): أبعاد ومؤشرات الشمول المالي

البعد	المفهوم	بعض مؤشرات القياس
الوصول إلى الخدمات المالية	تشير إلى القدرة على استخدام الخدمات المالية من مؤسسات الرسمية، ولتحديد مستويات الوصول يجب تحديد وتحليل العوائقق المحتملة لفتح واستخدام حساب مصرفي.	▪ عدد نقاط الوصول لكل10،000 من البالغين على المستوى المحلي بحسب المحافظة. ▪ عدد أجهزة الصراف الآلي لكل 1000كلم.^{2} ▪ حسابات التحويل المالي الإلكتروني. ▪ إمكانية الترابط بين نقاط تقديم الخدمة. ▪ النسبة المئوية لإجمالي السكان الذين يعيشون في المحافظة بنقطة وصول واحدة على الأقل.
استخدام الخدمات المالية	تشير إلى مدى استخدام العملاء للخدمات المالية المقدمة بواسطة مؤسسات القطاع المصرفي، ولتحديد مدى الاستخدام يجب جمع بيانات حول مدى انتظام وتواتر الاستخدام عبر فترة زمنية معينة.	▪ نسبة البالغين الذين لديهم نوع واحد على الأقل كحساب وديعة منتظم. ▪ نسبة البالغين الذين لديهم نوع واحد على الأقل كحساب ائتمان منتظم. ▪ عدد المتعاملين بسياسة التأمين لكل1000 من البالغين. ▪ عدد معاملات التجزئة غير النقدية للفرد الواحد. ▪ عدد معاملات الدفع عبر الهاتف. ▪ – نسبة الشركات (ض أو م) التي لديها حسابات رسمية مالية.
جودة الخدمات المالية	يشير إلى مدى ملائمة الخدمة أو المنتج المالي لاحتياجات ونمط حياة المستهلك.	▪ القدرة على تحمل التكاليف. ▪ الشفافية. ▪ حماية المستهلك. ▪ الراحة والسهولة. ▪ التثقيف المالي.

المصدر: (سفاري و بن داية، 2021، صفحة 75)

4- أهمية الشمول المالي:

الشمول المالي هو عبارة عن إستراتيجية طويلة المدى ولكن لتحقيق أهداف هذه إستراتيجية يمكن الأخذ بعين الاعتبار المجالات الرئيسية التي يجب أن يتناولها الشمول المالي (شنبي و بن لخضر، 2019):

- تكشف مجموعة متزايدة من البحوث أن هناك منافع إنمائية عديدة يمكن تحقيقها من الشمول المالي، لاسيما من استخدام الخدمات المالية الرقمية بما فيها الخدمات المالية عبر الهواتف المحمولة، وبطاقات الدفع، وغيرها من تطبيقات التكنولوجيا المالية.
- تحقيق منافع واسعة النطاق من الشمول المالي، حيث أظهرت الدراسات أن الخدمات المالية عبر الهاتف المحمول تسمح للمستخدمين بحفظ الأموال وتحويلها وبالتالي تساعد في تحسين إمكانيات كسب الدخل، والحد من الفقر.
- يمكن للخدمات المالية الرقمية أيضا أن تساعد الناس على إدارة المخاطر المالية من خلال تسهيل جمع الأموال من الأصدقاء والأقارب البعيدين في الأوقات الصعبة.
- تساعد الخدمات المالية الناس على تراكم المدخرات وزيادة الإنفاق على الضروريات.
- بالنسبة للحكومات، فالتحول من المدفوعات النقدية إلى الرقمية يمكن أن يقلل من الفساد ويحسن مستوى المعيشة.

ثانيا: الأمن السيبراني

تشهد العديد من دول العالم تحولا كبيرا في قطاعاتها المالية، مع قيامها بتوسيع نطاق الشمول المالي والتحول إلى الخدمات المالية الرقمية (مورر و آثرنيلسون، 2021)، كما شهد هذا القطاع سلبيات هذا التحول مع تزايد حجم وتعقيدات الهجمات السيبرانية، وأصبح الأمن السيبراني مصدر قلق كبير في كافة أنحاء العالم، وتزايد الاهتمام العالمي بالأمن السيبراني. فما هو الأمن السيبراني وما هي أشكال تهديداته وأهميته في القطاع المالي؟

1- تعريف الأمن السيبراني:

تناولت العديد من الأبحاث موضوع الأمن السيبراني، ومن بين التعريفات الواردة فيه أنه "حماية الفضاء السيبراني من الوصول إليه دون تصريح أو سوء استخدام، بما في ذلك الاعتداء المتعمد أو بطريق الخطأ أو نتيجة الإخفاق في إتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي إلى ذلك".

ويعرف **الفضاء السيبراني** بأنه "بيئة تتكون من تفاعل الأشخاص والبيانات والمعلومات ونظام المعلومات والبرامج على الشبكات المعلوماتية وأنظمة الاتصالات والبنى التحتية المرتبطة بها".

كما يعرف على انه "ممارسة حماية أجهزة الكمبيوتر والشبكات وتطبيقات البرامج والأنظمة الهامة والبيانات من التهديدات الرقمية المحتملة" (cisco، 2023).

وعرف الاتحاد الدولي للاتصالات الأمن السيبراني بأنه "مجموعة من الأدوات والسياسات والمفاهيم الأمنية وضمانات الأمان والمبادئ التوجيهية، وأساليب إدارة المخاطر، والإجراءات والتدريب، وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدم" (بارة، 2017).

ويتضمن الأمن السيبراني تقنيات وممارسات مصممة لحماية الشبكات والأجهزة من الهجوم والتلف من أي وصول غير مصرح به.

2- تعريف وأشكال تهديدات الأمن السيبراني على القطاع المالي

يمكننا تعريف التهديدات السيبرانية بكونها "التهديدات والمخاطر التي تواجه المستخدمين مهما كان نوعهم سواء أفراد أو جماعات أو غيرها على الانترنت"، وقد يكون التهديد من قبل أشخاص أو مجموعات أو مؤسسات، تهدف بشكل أساسي لإلحاق الأذى والتدمير والتخريب على الهدف الذي تم استهدافه، حيث تختلف الأهداف فقد تكون تخريبية أو سرقة أو ابتزاز وغيرها.

هذا.وبالنسبة لأشكال تهديدات الأمن السيبراني فإن أكبر تهديدات الأمن السيبراني على القطاع المالي هي (معاد، هل يمكن لويندوز 11 تلبية متطلبات الأمن السيبراني للبنوك والمؤسسات؟، 2022):

- **البيانات غير المشفرة:** أحد التهديدات الشائعة التي تواجهها البنوك هو عندما تُترك البيانات غير مشفرة، ويستخدم المتسللون أو مجرمو الإنترنت البيانات على الفور، مما يتسبب في مشكلات خطيرة يجب أن تكون جميع البيانات المخزنة على أجهزة الكمبيوتر في البنوك والمؤسسات أو عبر الإنترنت مشفرة بالكامل، مما يضمن أنه حتى في حالة سرقة البيانات، فقد لا يتمكن مجرمو الإنترنت من استخدام هذه البيانات.
- **البرامج الضارة:** تُستخدم أجهزة الكومبيوتر والأجهزة المحمولة في الغالب لإجراء المعاملات الرقمية مما يستوجب تزويدها بالحماية. وتشكل البرامج الضارة خطراً كبيراً على البنوك عندما تتم المعاملات عبر الشبكات الالكترونية والانترنت، تمر البيانات الحساسة عبر الشبكات الالكترونية والانترنت، وإذا كان جهاز المستخدم يحتوي على برامج ضارة مثبتة فيه دون أي حماية يمكن أن تشكل البرامج الضارة تهديداً خطيراً لشبكة البنك.
- **خدمات الطرف الثالث:** تلجأ العديد من البنوك والمؤسسات إلى الجهات الخارجية من البائعين وغيرهم (خدمات الطرف الثالث) بهدف خدمة عملائهم بشكل أفضل، وإذا لم يكن لدى هؤلاء الجهات الخارجية إجراءات صارمة للأمن السيبراني، فقد يواجه البنك مشاكل أمنية من خدمات الطرف الثالث.
- **الانتحال:** إنه أحد أحدث أشكال التهديدات الإلكترونية التي تواجهها البنوك، حيث ينتحل مجرمو الإنترنت عنوان موقع المصرف على الويب URL بموقع ويب مشابه للموقع الأصلي ويعمل بالطريقة عينها، وعندما يقوم المستخدم بإدخال بيانات تسجيل الدخول الخاصة به على الموقع المزيف، يتم سرقة بيانات تسجيل الدخول من قبل هؤلاء المجرمين واستخدامها لاحقاً. وتتزايد حدة هذا التهديد مع استخدام تقنيات انتحال جديدة من قبل مجرمي الإنترنت.

- **التصيد الاحتيالي:** التصيد الإحتيالي هو محاولة الحصول على معلومات حساسة مثل تفاصيل بطاقة الائتمان عن طريق التنكر ككيان جدير بالثقة في إتصال إلكتروني، وتتطور عمليات التصيد الإحتيالي على الإنترنت بشكل مستمر.

3- أهمية الأمن السيبراني في القطاع المالي:

أدى التسارع الكبير في تبني البنوك التقنيات الرقمية الحديثة لتحسين الخدمات المالية لتوسيع الشمول المالي مواكبة التغيرات والتطورات العالمية إلى تزايد الهجمات السيبرانية عليها، لهذا استوجب عليها الاهتمام بتدابير الأمن السيبراني، لأنها تحقق الفوائد التالية:

- الإبقاء على درجة نزاهة وثقة مرتفعة، مما يُعزز من ثقة عملائها بها وينعكس إيجابيا على سمعتها.
- تجنّب عقوبات عدم الامتثال، بالالتزام بمجموعة من القواعد والقوانين لتتعامل مع التهديدات التي تتعرض لها، وتضمن سلامة بيانات عملائها.
- منع الخسائر المالية التي تتعرض لها البنوك جراء تهديدات الأمن السيبراني.
- حماية بيانات البنوك من الانتهاك والاختراق ويحمي أموال العملاء.

4- تحديات الأمن السيبراني في القطاع المالي:

يعتبر الأمن السيبراني تحديا خطيرا بالنسبة للقطاع المالي بسبب التوجه السريع نحو التحول الرقمي بهدف تحسين جودة الخدمات المالية وزيادة فرص الوصول المالي ضمن إستراتيجية تعزيز الشمول المالي وتتمثل هذه التحديات في العوامل التالية (معاد، هل يمكن لويندوز 11 تلبية متطلبات الأمن السيبراني للبنوك والمؤسسات؟، 2022):

- **نقص الوعي:** إن الوعي لأهمية الأمن السيبراني بين الناس منخفضاً للغاية، ولا تستثمر العديد من الشركات في التدريب وتحسين الوعي العام بالأمن السيبراني.
- **الميزانيات غير الكافية والافتقار إلى الإدارة:** يُمنح الأمن السيبراني أولوية وميزانية منخفضة غالباً، ولا يزال تركيز الإدارة العليا على الأمن السيبراني منخفضاً في معظم البنوك، وتُعطى مشاريع الأمن السيبراني أولوية منخفضة. قد يكون هذا لأن الإدارة العليا لا تكترث لتأثير تهديدات الأمن السيبراني.
- **ضعف أمن هوية الدخول والوصول الى الشبكات:** إن إدارة هوية الدخول والوصول إلى الشبكات الإلكترونية هي العنصر الأساسي في الأمن السيبراني إذ أن اختراق واحد لهوية الدخول والوصول إلى الشبكة كاف لاختراق كل شبكة البنك وإلحاق الضرر بها.
- **زيادة برامج الفدية Ransomware:** يتزايد خطر برامج الفدية حيث بدأ مجرمو الإنترنت في استخدام الأساليب التي تتجنب اكتشافهم بالتركيز على الملفات القابلة للتنفيذ ووضع الضرر فيها.
- **الأجهزة المحمولة والتطبيقات:** اعتمدت معظم المؤسسات المصرفية الهواتف المحمولة كوسيلة لإجراء الأعمال، ومع زيادة قاعدة استخدام الأجهزة المحمولة وارتفاع حجم المعاملات عبرها، تصبح هذه الأجهزة هدفاً للمتسللين.

II - الجزء التطبيقي :

يعتبر على نطاق واسع فتح حساب مالي الخطوة الأولى نحو الشمول المالي، لهذا ركزنا على نمو ملكية الحسابات المالية للبالغين وامكانية الوصول المالي لزيادة فرص الشمول المالي كأهم مؤشرات لمعرفة مكاسب الشمول المالي وأهم عوامل التحول الرقمي التي ساهمت في ذلك بالإعتماد على بيانات قاعدة المؤشر العالمي للشمول المالي إصدار 2021، كما سننتطرق إلى احصائيات التهديدات السيبرانية وبعض الأمثلة عنها، ومجهودات الدول لتقوية أمنها السيبراني وفي الأخير نعرض آليات التحوط التي توصلت إليها أهم الهيئات الدولية، واللجنات الإشرافية والمؤسسات المالية لتقوية الأمن السيبراني لحماية مكاسب الشمول المالي.

أولا: مكاسب الشمول المالي التي حققها التحول الرقمي:

تشمل هذه المكاسب في مايلي:

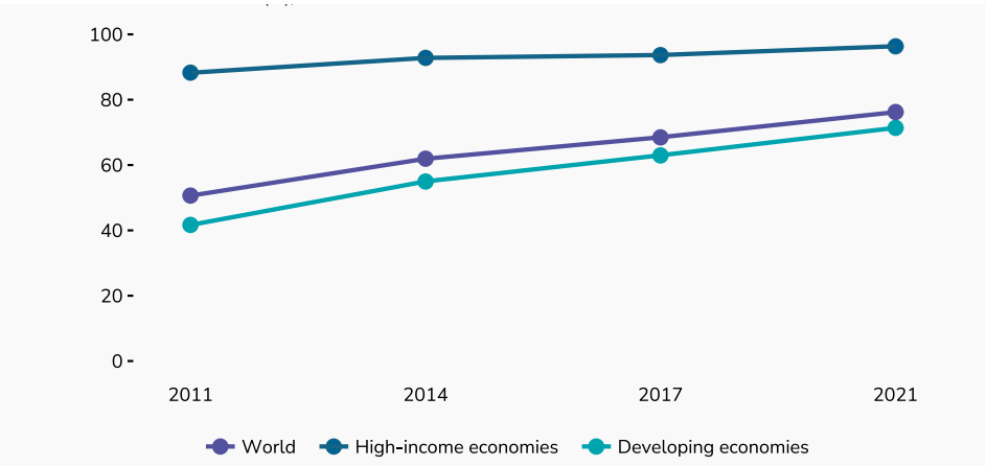
1- زيادة ملكية الحسابات المالية:

ملكية الحسابات هي المقياس الأساسي للشمول المالي، وأصحاب الحسابات أكثر قدرة على تجنب الإنزلاق في الفقر، لأنهم يجدون من الأسهل الإعتماد على المدخرات، أو تلقي الموارد المالية من اللأصدقاء أو العائلة في حالة الطوارىءالمالية، مثل فقدان الدخل.

عالميا، زادت ملكية الحسابات من 51% إلى 76% بين2011 إلى 2021 أي بنسبة زيادة قدرها 50%، وكان متوسط معدل النمو في الاقتصادات النامية أكثر حدة بشكل عام، نمت ملكية الحسابات في الاقتصاديات النامية ب30نقطة مئوية، من42% في 2011 إلى 71 % في 2021 بزيادة أكثر من 70%. وعلى الرغم من أن ملكية الحسابات شبه شاملة في العديد من الاقتصاديات ذات الدخل المرتفع منذ 2011، إلا أن متوسط الملكية زاد بمقدار 8نقاط مئوية ، من 88%في سنة2011 إلى 96% في عام2021.

الشكل (1): نسبة البالغين الذين لديهم حساب مالي من 2011-2021

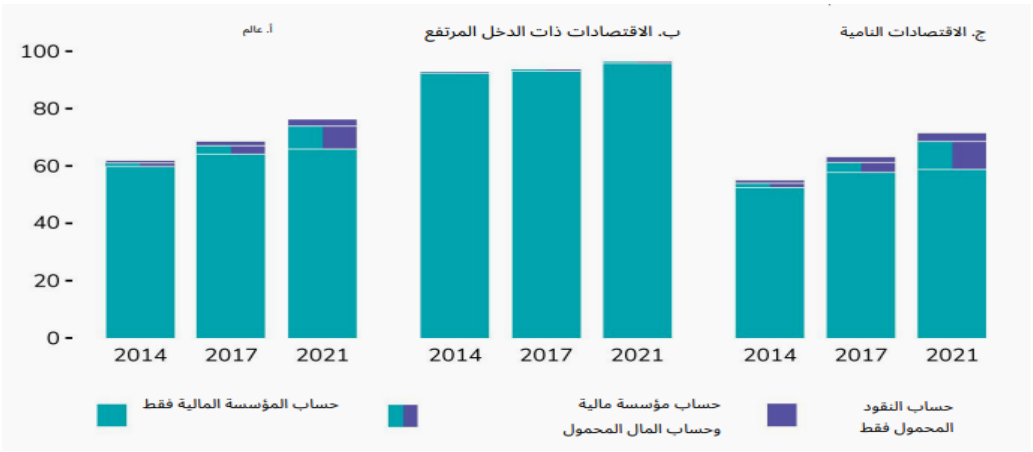
على مستوى العالم، وصلت نسبة ملكية الحسابات الى 76% من البالغين، و71% من البالغين في الاقتصادات النامية.



المصدر: TheGlobal FindexDatabase2021

كما يوضح الشكل (2) مساهمة حسابات الأموال عبر الهاتف المحمول في زيادة قدرها 8نقاط مئوية في ملكية الحسابات في الاقتصاديات النامية من 2014 إلى 2021.

الشكل (2): مساهمة حسابات الأموال عبر الهاتف المحمول في زيادة ملكية الحسابات المالية



المصدر:TheGlobal FindexDatabase2021

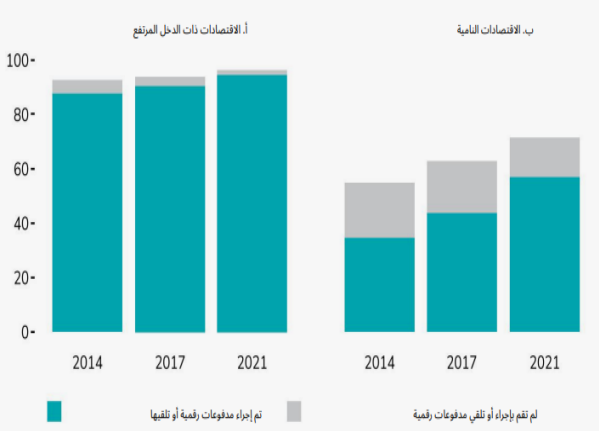
2- زيادة االمدفوعات الرقمية

تشمل المدفوعات الرقمية إستخدام حساب الأموال عبر الهاتف المحمول أو بطاقة الخصم أو الإئتمان، أو إجراء عملية الدفع من خلال الهاتف المحمول أو الأنترنيت لإرسال الاموال إلى الأقارب أو الأصدقاء، أو لدفع الفواتير، تشمل المدفوعات الرقمية أيضا مدفوعات التجار في المتجر أو عبر الانترنيت، ودفع فواتير المياه والكهرباء و إرسال أو إستقبال الحوالات المالية المحلية، تلقي مدفوعات للمنتجات الزراعية، أو تلقي أجور أو تحولات حكومية، أو معاش تقاعدي عام مباشرة من أو إلى حساب.

وفي استطلاع Global Findex 2021 قام 64%من84% مالكي الحسابات البالغين حول العالم بإجراء أو تلقي دفعة رقمية واحدة على الأقل في عام 2021، وفي الاقتصاديات ذات الدخل المرتفع، فعل ذلك 95% من98% أصحاب الحسابات البالغين، مقارنة ب57%من 80%من أصحاب الحسابات البالغين في الدول النامية، أنظر الشكل (3)اللوحة –أ- في الدول المتقدمة أصبح استخدام المدفوعات الرقمية شاملا لكل السكان تقريبا منذ سنة 2014، زادت حصة أصحاب الحسابات الذين يقومون بإجراء أو تلقي مدفوعات رقمية ارتفاعا من 63% عام 2014 %و69%عام 2017 إلى 80% في عام 2021.

وفي اللوحة – ب- في اقتصاديات الدول النامية نمت نسبة البالغين الذين قامو باجراء أو تلقي المدفوعات الرقمية بسرعة في السنوات الأخيرة وارتفعت بنسبة 13 نقطة مئوية بين عامي 2017 و2021 من 44%إلى 57% وفي عام 2014 كانت الحصة 35%.في الواقع فاق النمو في استخدام المدفوعات الرقمية النمو في ملكية الحسابات في الاقتصاديات النامية.

الشكل(3): نسبة البالغين الذين يستخدمون المدفوعات الرقمية خلال الفترة 2014 –2021



المصدر: TheGlobal FindexDatabase2021

3- زيادة فرص ملكية الحسابات:

على الصعيد العالمي، لقد سرع التحول الرقمي للقطاع المالي نفاذ الخدمات المالية الرقمية مما أدى إلى إستقطاب 3 مليار بالغ في الفترة 2017-2021,كما عززت جائحة كوفيد-19 هذا النمو السريع نظرا لما فرضتة من قيود، ولا يزال حوالي 1.4مليار بالغ لا يتعاملون مع البنوك – أي ليس لديهم حساب في مؤسسة مالية أو من خلال مزود خدمة الأموال عبر الهاتف، ولقد انخفض هذا الرقم من 2.5مليار في عام 2011 و1.7مليار في عام 2017، نظرا لأن ملكية الحسابات أصبحت عامة تقريبا في الإقتصادات ذات الدخل المرتفع، فإن جميع البالغين الذين لا يتعاملون مع البنوك تقريبا يعيشون في الإقتصادات النامية ويمتلك أكثر من نصفهم هاتفا محمولا مما يمثل فرصة لزيادة معدلات ملكية الحسابات عن طريق جذب هذه الطبقة المهمشة بزيادة مرونة المعاملات المالية الرقميةكما توضح الخريطة (2).

خريطة (2):البالغون بدون حساب حول العالم

المصدر: TheGlobal FindexDatabase2021

كشف هذه النتائج خاصة بعد أزمة كوفيد-19عن فرص جديدة لدفع الشمول المالي من خلال زيادة ملكية الحسابات بين غير المتعاملين مع البنوك وتوسيع استخدام الخدمات المالية بين أولئك الذين لديهم بالفعل حسابات لا سيما من الاستفادة من المدفوعات الرقمية من خلال الانتشار الواسع لاستخدام الانترنيت والهواتف المحمولة.

ثانيا: إحصائيات تهديدات الأمن السيبراني

❖ **الهجمات السيبرانية**

الشكل (4):تصاعد الهجمات السيبراني

المصدر: (جينكسون و إليوت، 2020)

خلال الفترة (2005-2020) يتعرض القطاع المالي لهجمات الكترونية واسعة النطاق، وازدادت حدتها بسبب زيادة مستخدمي الانترنيت وانتشارها على مستوى العالم، فضلا عن التوسع في استخدام المدفوعات الرقمية وانتشار شركات التكنولوجيا المالية،حيث تشير دراسة لصندوق النقد الدولي أن عدد الهجمات السيبرانية تضاعفت ثلاث مرات على مدار العقد الماضي، ولا تزال الخدمات المالية هي الأكثر استهدافا منها،كما أن تقديرات البنك الدولي تشير أيضا إلى أن قطاع الخدمات المالية يشهد هجمات سيبرانية تفوق القطاعات

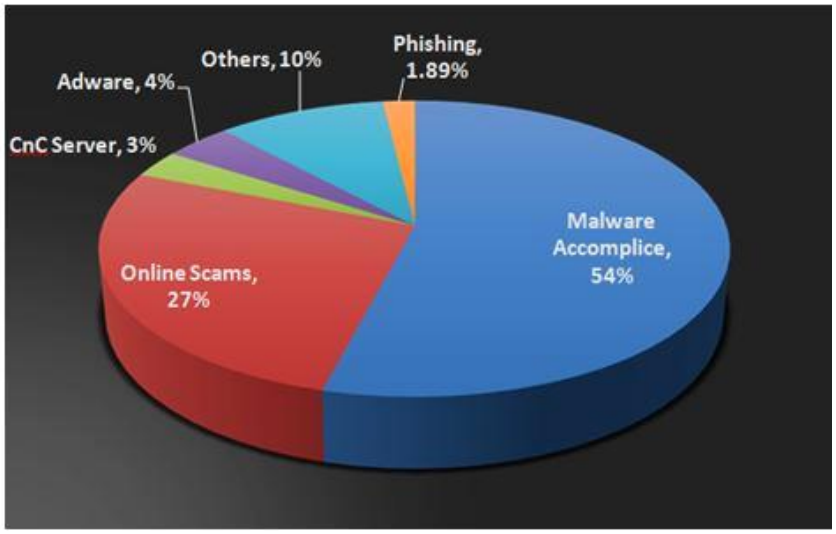
الأخرى بنسبة 65%، وقد أصبحت أدوات القرصنة الآن أقل تكلفة وأكثر سهولة وأشد قوة، مما يتيح للقراصنة ذوي المهارات المحدودة إلحاق ضرر أكبر مقابل نسبة ضئيلة من التكلفة السابقة. ويؤدي التوسع في الخدمات القائمة على الأجهزة المحمولة (وهي المنصة التكنولوجية الوحيدة المتاحة للكثيرين) إلى زيادة فرص القرصنة. ويستهدف المهاجمون المؤسسات كبيرها وصغيرها والبلدان سواء الغنية أو الفقيرة، ويعملون عبر الحدود.

❖ جرائم الاحتيال الإلكترونية:

وفقا للتقرير الذي أصدرته منظمة الشرطة الجنائية الدولية ''الإنتربول "**INTERPOL** بشأن تقييم تهديدات الجرائم السيبرانية في قارة أفريقيا للعام 2021، تعد جرائم الاحتيال عبر الإنترنت هي أهم التهديدات السيبرانية المنتشرة عبر القارة، وخاصة أخطارها المتعلقة بخدمات البنوك وبطاقات الائتمان، نظرًا لتضمنها اختراق أمن معلومات المؤسسات البنكية والوصول لبيانات العملاء الشخصية بما يُمكِّن المجرم من إجراء تحويلات أو إجراء عمليات شراء باستخدام البيانات (فتحي، 2021).

لقد شهدت القارة ارتفاع في ذلك النوع من العمليات خاصة وغيرها من التهديدات السيبرانية بشكل عام كأثر مباشر لجائحة ''كوفيد19'' قُدر بنسبة 238%، بينها العديد من فيروسات حصان طروادة**Trojan Virus** مثل **Tesla**و **Lokibot**و**Fareit** التي تحتوي على برمجيات ضارة **Malware** المخصصة للاحتيال الإلكتروني، كما يُعرض العديد من هؤلاء المجرمين أدوات للبيع تساهم في تسهيل تنفيذ الجرائم حتى على غير المحترفين وهو ما ساهم في اتساع دائرة مرتكبي ذلك النوع من الجرائم وضحاياها على حد سواء، وأوضح مركز معلومات المخاطر المصرفية في جنوب أفريقيا(**SABRIC**) أن إجمالي خسائر جرائم الاحتيال الخاصة ببطاقات الائتمان المصدرة من البنوك زادت بنسبة 20.5% بين عامي 2018 و2019 (فتحي، 2021).

الشكل(5):نسب التهديدات السيبرانية على القطاع المالي في قارة إفريقيا



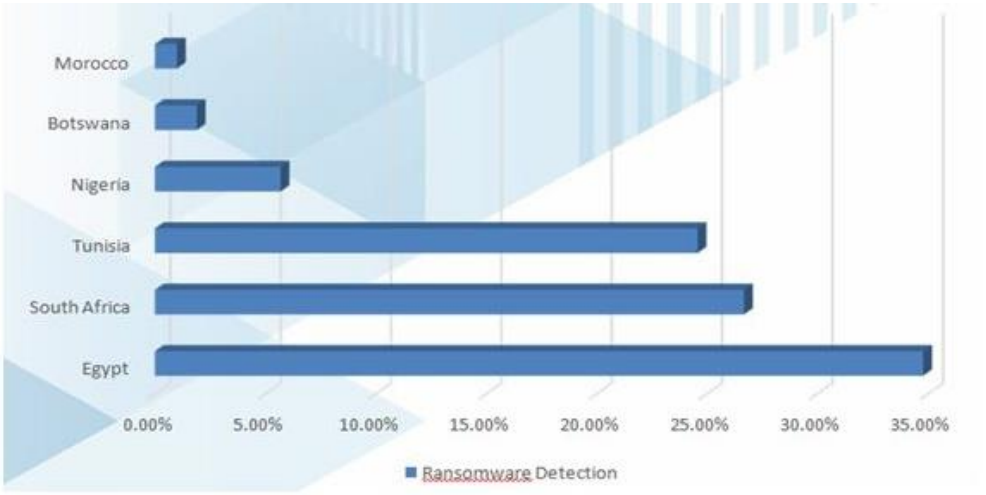
المصدر: (فتحي، 2021)

ووفقًا لإحصائيات الشركة الأمريكية اليابانية لبرمجيات الأمن السيبراني ''تريند مايكرو "**Trend Micro** في الشكل السابق فإن جرائم الاحتيال الإلكترونية شكلت نسبة 27% من التهديدات السيبرانية على مستوى قارة أفريقيا بالكامل حتى شهر مايو 2021، والجدير بالذكر أن الإحصائية فصلت برمجيات الإعلانات**Adware** بالرغم من عدم تعدي نسبتها لـ4% إلا أن تلك النسبة الصغيرة مقارنة بنسبة البرمجيات الضارة الكبيرة المقدرة بـ54% تشير إلى احتمالية كون برمجيات الإعلانات المكتشفة أو العلنية فقط هي ما تمثل . نسبة4% (فتحي، 2021).

❖ **برامج الفدية:**

ويُظهر البحث الذي أجرته شركة **Kaspersky** أن هناك أكثر من 1.5 مليون عملية اكتشاف لبرامج الفدية في عام 2020، وفي الربع الأول من عام 2021 عانت مصر وجنوب أفريقيا وتونس من أعلى نسبة اكتشاف على مستوى قارة أفريقيا، وأن مصر وحدها تمثل ما يقرب من 35% من جميع عمليات اكتشاف برامج الفدية في أفريقيا (فتحي، 2021).

الشكل(6): إحصائيات برامج الفدية الضارة في إفريقيا في مارس 2021.



المصدر: (فتحي، 2021)

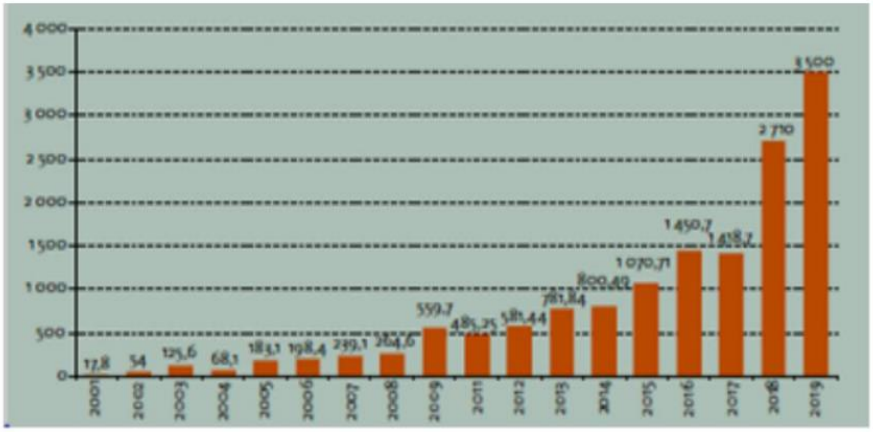
وعلى الرغم من أن نسبة اكتشافات برامج الفدية الإجمالية في أفريقيا احتلت المرتبة الأدنى 10% مقارنة بجميع المناطق الأخرى، إلا أن بحث من **Check Point Software Technologies** قد أفاد بأن المنظمات الأفريقية شهدت أعلى زيادة في الهجمات بنسبة 34%، من يناير إلى أبريل 2021 وفقًا لمركز أفريقيا للدراسات الاستراتيجية في يناير 2021 ، مع زيادة انتشار الإنترنت وزيادة ارتباط الأنظمة فمن المرجح أن تتعرض البنية التحتية الحيوية في جميع أنحاء القارة أكثر لهجمات إلكترونية مدمرة ومكلفة، و **Nefilim ransomware** الأحدث والأسوأ سمعة، والذي يستهدف المؤسسات المصرفية في أفريقيا الذي اكتشف في مارس 2020.

نظرًا لسعي مجرمي برامج الفدية لتحقيق أرباح فسوف تستمر المشكلة على مستوى العالم طالما أن المنظمات الضحية مستعدة لدفع الفدية أو مجبرة على ذلك، وقد توقع معهد "بروكنجز **Brookings**" أن تتفاقم التهديدات الإلكترونية في أفريقيا في مارس 2021 بسبب نقاط الضعف في استراتيجيات الأمن السيبراني العامة والآثار الاقتصادية لوباء COVID-19.(فتحي، 2021).

❖ **الخسائر الإقتصادية الناتجة عن التهديدات السيبرانية**

تتزايد الخسائر المالية الناجمة عن التهديدات السيبرانية مع زيادة التوجه نحو التحول الرقمي وخاصة في البلدان النامية حديثة التجربة، وقد وصلت في عام 2019 إلى 3500 مليار دولار (اسماعيل، 2019) لتصل إلى 6 ترليون دودولار في سنة 2021، وفقا لتقديرات الإتحاد الدولي للإتصالات (الأردن، 2021). وتتوقع دراسة مشروع الأمن السيبراني أن تزداد تكالف الهجمات السيبرانية بنسبة 15%سنويا، لتصل إلى 10.5ترليون دولاربحلول عام 2025 (Laib, 2021).

الشكل (7): الخسائر الاقتصادية الناتجة عن التهديدات السيبرانية



المصدر: (Laib, 2021)

ثالثا: آليات التحوط من التهديدات السيبرانية على القطاع المالي

تهدّد الهجمات السيبرانية الاستقرار الاقتصادي بسبب زيادة الاتّصال بين القطاعين المالي والتّكنولوجي، فالهجمات على المؤسّسات المالية الكبرى أو النظام الأساسي أو الخدمات التي تعتمدها تؤدي إلى تداعي النظام المالي بأسره، مما يتسبب في فقدان الثقة بالإضافة إلى فشل المعاملات وحبس السيولة، وإعاقة عمل الشّركات. وتؤدّي الهجمات السيبرانية كذلك إلى إعاقة قدرة المؤسّسات المالية عن النّفاذ إلى الودائع والمدفوعات، مما تنتج عنه نتائج سيئة مثل مطالبة المستثمرين والمودعين بأموالهم أو إلغاء حساباتهم والمغادرة (المعلومة بتقنية، 2023). ونتيجة لذلك واعترافا بالتهديدات الناجمة عن المخاطر السيبرانية, ومدى أهمية تعزيز قدرة الأجهزة المصرفية على تحمل هذه المخاطر والتحوط منها, فقد اتخذت السلطات الرقابية على مستوى العالم خطوات تنظيمية وإشرافية تهدف إلى تجنب أثر المخاطر السيبرانية على القطاع المالي (اسماعيل، 2019), وفي ما يلي أهم آليات التحوط من التهديدات السيبرانية لحماية القطاع المالي ومنه انجازات الشمول التي حققها التحول الرقمي.

المرونة السيبرانية: تعزز المرونة السيبرانية الدفاع الجماعي لحماية القطاع المالي من التهديدات السيبرانية, وفي العام 2021 ، دعت لجنة بازل للرقابة المصرفية البنوك إلى تحسين قدرتها على الصمود أمام التهديدات السيبرانية، ورفع مستوى المرونة السيبرانية. كما يرى المنتدى الاقتصادي العالمي، أن الأمن السيبراني لم يعد كافياً لحماية المؤسسات من الهجومات السيبرانية المستمرة. وهناك حاجة ملحة إلى المرونة السيبرانية (معاد، المرونة السيبرانية وفق بازل، 2022).

والمرونة السيبرانية هي قدرة المؤسسة على الاستعداد والتعامل مع التهديدات السيبرانية والتعافي منها.

إعداد الخرائط السيبرانية والتحديد الكمي للمخاطر: يمكن الخروج بفهم أفضل لأوجه الاعتماد المتبادل في النظام المالي العالمي عن طريق إعداد خرائط لأهم الروابط التشغيلية والتكنولوجية المتبادلة والبنية التحتية ذات الأهمية الحرجة (جينكسون و إليوت، 2020).

تقارب القواعد التنظيمية: ستؤدي زيادة الاتساق الدولي في مجال التنظيم والرقابة إلى تخفيض تكاليف الامتثال وبناء منبر لتعاون أقوى عبر الحدود. وقد بدأت جهود تعزيز التنسيق وزيادة التقارب من جانب جهات دولية، مثل مجلس الاستقرار المالي ولجنة المدفوعات والبنى التحتية للأسواق المالية ولجنة بازل. وينبغي للسلطات الوطنية أن تعمل معا من أجل التنفيذ (جينكسون و إليوت، 2020).

القدرة على الاستجابة: في ظل شيوع الهجمات السيبرانية بشكل متزايد، يجب أن يكون النظام المالي قادرا على استئناف عملياته بسرعة حتى في مواجهة هجمة ناجحة (جينكسون و إليوت، 2020).

الرغبة في العمل المشترك: من شأن زيادة تبادل المعلومات بشأن التهديدات والهجمات والاستجابات عبر القطاعين العام والخاص أن تعزز القدرة على الردع والاستجابة بشكل فعال (جينكسون و إليوت، 2020).

ردع أقوى: ينبغي أن تصبح الهجمات السيبرانية أكثر تكلفة وخطرا من خلال إجراءات فعالة لمصادرة عائدات الجريمة ومقاضاة المجرمين. ومن شأن تعزيز الجهود الدولية لمنع المهاجمين وتعطيلهم وردعهم أن يقلص المخاطر من منبعها. ويتطلب هذا تعاونا وثيقا بين أجهزة إنفاذ القانون والسلطات الوطنية المسؤولة عن البنية التحتية الحيوية أو عن الأمن، عبر البلدان والهيئات المعنية. ولما كان القراصنة لا يعترفون بالحدود، فإن مواجهة الجريمة العالمية تتطلب إنفاذا عالميا للقوانين المتفق عليها (جينكسون و إليوت، 2020).

محو الأمية التقنية المالية ونشر الوعي الرقمي: إعداد برامج الأمية المالية بما يحقق الفائدة والمنفعة للأفراد تحت مظلة الشمول المالي. كما يجب توفير الدعم الفني لمستخدمي التطبيقات الرقمية خاصة المبتدئين، وهذا من أجل كسب ثقة المواطن وضمان ولائه (دراعو، 2022).

الحلول التقنية: تعتمد أساسا على اعتماد كلمة سر قوية صعبة الإختراق وتغييرها بصفة دورية, كما يتعين استخدام تقنية التوقيع الرقمي لدى المصارف وشركات البطاقات الائتمانية (دراعو، 2022).

تنمية القدرات: ستؤدي مساعدة الاقتصادات النامية والصاعدة على بناء القدرات في مجال الأمن السيبراني إلى تعزيز الاستقرار المالي ودعم الشمول المالي. والبلدان منخفضة الدخل معرضة بشكل كبير للمخاطر السيبرانية. وقد أبرزت أزمة جائحة كوفيد-19 الدور الحاسم الذي يقوم به الربط الإلكتروني في العالم النامي. وستظل الاستفادة من التكنولوجيا بشكل يحفظ الأمن والسلامة قضية محورية في التنمية ومعها الحاجة إلى ضمان معالجة المخاطر السيبرانية. وعلى غرار أي فيروس، فإن تكاثر التهديدات السيبرانية في أي بلد يجعل بقية العالم أقل أمانا (جينكسون و إليوت، 2020).

الإلتزام بتدابير الأمن السيبراني: يعد المؤشر العالمي للأمن السيبراني (GCI) الذي يصدر عن الاتحاد الدولي للاتصالات التابع رسميا للأمم المتحدة، مرجعاً موثوقاً به يقيس التزام الدول بالأمن السيبراني على المستوى العالمي, ويرصد المؤشر التحسن في مستويات الوعي بأهمية الأمن السيبراني, والتدابير المتخذة لحمايته في 193دولة من دول العالم استنادا إلى عدة مقومات عبر خمسة أركان أساسية ، وتتمثل في: التدابير القانونية، التدابير التقنية، التدابير التنظيمية، والتدابير الرامية إلى بناء القدرات في مجال حماية الأمن السيبراني ، وأخيرا التي تهدف إلى تعزيز التعاون في هذا الشأن (أبوغزالة، 2021) .كما يدعم الرقم القياسي العالمي للامن السيبراني البلدان في تحديد مجالات التحسين في ميدان الأمن السيبراني، وتحفيزها من أجل اتخاذ إجراءات لتحسين ترتيبها، وهو ما يؤدي بدوره إلى زيادة المستوى العام للأمن السيبراني في العالم (السيبرانية، 2020).

الجدول(2): ترتيب الدول العشر الأوائل حسب المؤشر العالمي للأمن السيبراني سنة 2021

الترتيب عالميا	الدولة	العلامة	الترتيب عربيا	الترتيب عالميا	الدول العربية	العلامة
1	الولايات المتحدة الأمريكية	100	1	2	المملكة العربية السعودية	99.54
2	المملكة العربية السعودية	99.54	2	5	الإمارات	98.06
3	أستونيا	99.48	3	21	عمان	96.04
4	كوريا الجنوبية, سنغافورة,إسبانيا	98.52	4	23	مصر	95.48
5	الإمارات و روسيا, ماليزيا	98.06	5	27	قطر	94.5
6	ليتوانيا	97.93	6	45	تونس	86.23
7	اليابان	97.82	7	50	المغرب	82.41
8	كندا	97.67	8	60	البحرين	77.86
9	فرنسا	97.6	9	65	الكويت	75.05

10	الهند	97.5	10	71	الأردن	70.05

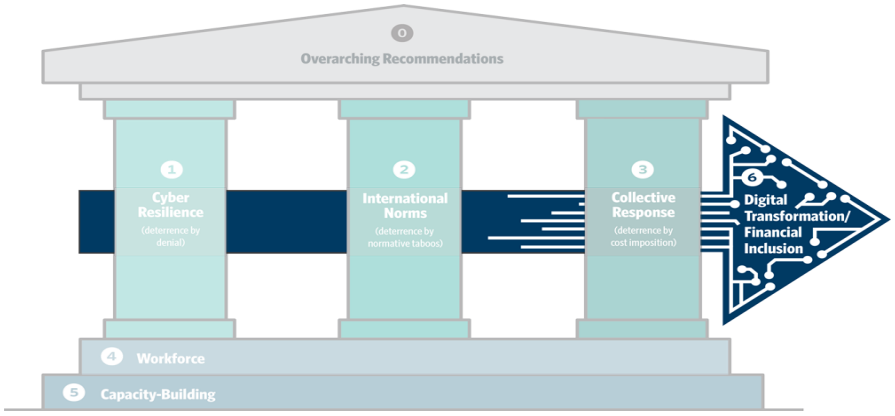
المصدر: من إعداد الباحثين بالاعتماد على (أجعاف، 2021)

ويبن الجدول أعلاه ترتيب الدول الرائدة في مجال الأمن السيبراني وتتصدرها الولايات المتحدة الأمريكية عالميا والسعودية الثانية عالميا والأولى عربيا ,أما الجزائر فقد حصلت على 33.95نقطة لتحتل بذلك المرتبة 104عالميا, وفي المنطقة العربية12 (صوت الجزائر، 2021). وهذا ما يعني ضعف الأمن السيبراني وعلى الهيئات المختصة أن تراعي هذا الجانب لأنه يدق ناقوس الخطر إلى تعرض دولتنا لمخاطر سيبرانية تهدد إستقرارها الاقتصادي والمالي والقانوني خصوصا ونحن في عصر التحول الرقمي.

وكل آليات التحوط السابقة الذكر فهي مترابطة فيما بينها لتقوية الأمن السيبراني لحماية النظام المالي بما فيه إنجازات الشمول المالي

حماية إنجازات الشمول المالي التي حققها التحول الرقمي: وتمثل حماية انجازات الشمول المالي التي حققها التحول الرقمي أولوية رقم (6)في مشروع كارنيجي "الإستراتيجية الدولية لحماية أفضل للنظام المالي العالمي ضد التهديدات السيبرانية". وتركز هذه الأولية على التحول الرقمي الهائل الذي يعيد تشكيل النظام المالي حاليا. يتمثل أحد المجالات التي تظهر فيها هذا التحول بشكل واضح في الجهود الكبيرة التي بذلتها مجموعة العشرين وأصحاب المصلحة الآخرون لتوسيع الشمول المالي في جميع أنحاء العالم وزيادة الوصول إلى الخدمات المالية الرقمية (DFS) وتغير مستوى ونوع الترابط بين النظام المالي وشركات التكنولوجيا. ولذلك فإن حماية إنجازات الشمول المالي ضد التهديدات السيبرانية المتزايدة يمثل تحديا ملحا(MAURER & NILSON, 2020) .

الشكل (8):العلاقة بين مجالات الأولوية لمشروع الإستراتيجية الدولية لحماية أفضل للنظام المالي العالمي ضد التهديدات السيبرانية



المصدر:(MAURER & NILSON, 2020)

III- الخلاصة :

يمكننا القول أن التحول الرقمي للقطاع المالي ساهم في تسريع وتيرة الشمول المالي, ولقد أكدت جائحة كوفيد -19 الحاجة الملحة لهذا التحول مما كان حلا للقيود المفروضة في خضم الجائحة , وساعد في وصول المساعدات المالية للطبقات المتضررة , لكن باالتوازي جلب مخاطرا سيبرانية جديدة, شكلت تهديدا متزايد على الإستقرار المالي والنظام المالي بأكمله , مما أدى بإعادة النظر في أستراتيجية التحول الرقمي للقطاع المالي لزيادة توسيع نطاق الشمول المالي وذلك بالتركيز على أهمية الأمن السيبراني في سياق الشمول المالي لحماية مكاسب الشمول المالي التي حققها التحول الرقمي ومجهودات مجموعة العشرين في تعزيز الشمول المالي كأحد أجندة التنمية المستدامة.

وتوصلت الدراسة إلى عدة نتائج أهمها:

- ✓ حقق التحول الرقمي للقطاع المالي شوطا كبيرا في زيادة معدلات الشمول المالي، ومازال هناك 1.4مليار مستبعدين ماليا؛
- ✓ ساهم الانتشار الكبير للانترنيت والإستخدام الواسع للهواتف المحمولة في زيادة ملكية الحسابات وخاصة في الدول النامية،

- ✓ بينت جائحة كوفيد- 19الدور الحاسم الذي يلعبة الرابط الإلكتروني والحاجة الملحة للخدمات المالية الرقمية؛
- ✓ أدى الإعتماد الكبير للقطاع المالي على الخدمات المالية الرقمية إلى زيادة التهديدات السيبرانية عليه؛
- ✓ يشكل الأمن السيبراني تحديا خطيرا للتحول الرقمي للقطاع المالي؛
- ✓ الأمن السيبراني لم يعد كافيا للتصدي للتهديدات السيبرانية بل أصبحت الحاجة ملحة للمرونة السيبرانية ؛
- ✓ يساعد مشروع بناء القدرات لصندوق النقد الدولي الدول النامية في تقوية أمنها السيبراني وخصوصا في مجال الشمول المالي؛

وأوصت الدراسة بما يأتي:

- ✓ يجب على الهيئات المعنية بالشمول المالي توعية العملاء بمخاطر الأمن السيبراني (لوزري، 2021)؛
- ✓ على الدول النامية كالجزائر التي تسجل رتبا متدنية في المؤشر العالمي للأمن السيبراني إعادة النظر في تدابير الأمن السيبراني لديها والإقتداء بالدول الرائدة في الأمن السيبراني؛
- ✓ يجب البحث عن الحلول التي توازن بين اختراعات التكنولوجيا المالية ومخاطر الأمن السيبراني دون الضرر بمكاسب الشمول المالي؛
- ✓ يجب توحيد الجهود الدولية في صد هذه الهجمات الإلكترونية وحماية النظام المالي العالمي؛
- ✓ يجب على الجامعات ومراكز البحث والتطوير التركيز أكثر على تخصص الأمن السيبراني؛
- ✓ يجب تدريب الإطارات في القطاع المالي على مواجهة مخاطر الأمن السيبراني والتدريب على المرونة السيبرانية؛

- الإحالات والمراجع :

(2015). *صندوق النقد العربي* ، صفحة 2.

Abdelfateh, a. M. (2018). Constriction d'unindice d'inclusion financière pour les payes Mombre de (OCi).

cisco. (13 03, 2023). تم الاسترداد من https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.html.

GROUP, W. B. *the Global Findex Database2021 Financial Introduction?*

Laib, S. (2021, June). The importance of cyber security in the financial sector in the age of digital transformation. *El-Acil Journal for Economic and Administraative Rescearch* .

TIM MAURER، و ARTHUR NILSON. (2020). *International Strategy to Better Protect the Finaancial system Against Cyber Threats*. CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE.

أسماء سفاري، و آسيا بن داية. (2021). تاثير تطبيق سياسة الشمول المالي على استقرار القطاع المصرفيك دراسة حالة الجزائر. *مجلة الاقتصاد الصناعي (خزراتك)* ، صفحة 75.

المعلومة بتقنية. (12 جانفي, 2023). تاريخ الاسترداد 23 أفريل, 23، من https//WWW.the8iog.com.

المنتدى العالمي للخبرات السيبرانية. (2020). *نظرة عامة على أدوات تقييم القدرات السيبرانية القائمة على الصعيد الوطني(GOAT)*.

الوليد طلحة، و الفران صبري. (ديسمبر, 2020). الشمول المالي الرقمي. *صندوق النقد الدولي* ، صفحة 3.

بنك الأردن. (2021).

تيم مورر، و آثرنيلسون. (مارس, 2021). التهديد السيبراني العالمي. *مجلة التمويل والتنمية* ، 25.

جهاد فتحي. (2021). *التهديدات السيبرانية بأفريقيا 2021...قراءة في تقرير الأنتربول*.

سمير بارة. (جويلية, 2017). الأمن السيبراني (CyberSecurity)في الجزائر: السياسات والمؤسسات. *المجلة الجزائرية للأمن السيبراني* ، صفحة 258.

سهى معاد. (2022). *المرونة السيبرانية وفق بازل*. اتحاد المصارف العربية.

سهى معاد. (2022). *هل يمكن لويندوز 11 تلبية متطلبات الأمن السيبراني للبنوك والمؤسسات؟* اتحاد المصارف العربية.

صندوق النقد العربي. (2021).

صوت الجزائر. (07 جويلية, 2021). تاريخ الاسترداد 28 04, 2023، من https://www.sawteldjazair.dz/.

صورية شنبي، و السعيد بن لخضر. (جانفي, 2019). أهميةالشمول المالي في تحقيق التنميية(تعزيز الشمول المالي في جمهورية مصر العربية). *مجلة البحوث في العلوم المالية والمحاسبية* .

عز الدين دراعو. (جوان, 2022). الآثار الاقتصادية والمالية للهجمات السيبرانية في ظل التحول الرقم: النتائج, التجارب والحلول- مع إشارة لحالة الجزائر-. *مجلة التكامل الاقتصادي* .

كوم خديجة أجعاف. (5 جويلية, 2021). تصنيف المغرب في المركز السابع عربيا وفي المرتبة الخمسين عالميا في مؤشر الأمن السيبراني. *برلمان* .

محمد أبوغزالة. (2021). تصدر الامارات المؤشرات العالمية في الأمن السيبراني ..الأهمية والدلالات والسياق. *ترينداز للبحوث والاستشارات* .

محمد اسماعيل. (2019). *الأمن السيبراني في القطاع المصرفي*. صندوق النقد العربي.

نادية لوزري. (ديسمبر, 2021). واقع الشمول المالي في الدول العربية وآليات تعزيزه- دراسة مقارنة لمستوى الشمول المالي في مجموعة الدول العربية-. *مجلة بحوث الاقتصاد والناجمنت* ، صفحة 15.

نايجل جينكسون، و جينفر إليوت. (2020). *الخاطر السيبرانية...التهديد الجديد للإستقرار المالي*.

كيفية الاستشهاد بهذا المقال حسب أسلوب APA:

جميلة جغل، عادل زقرير (2023)، **الأمن السيبراني والشمول المالي في ظل التحول الرقمي للقطاع المالي (التهديدات السيبرانية، اليات التحوط)**، مجلة التنمية الاقتصادية، المجلد 08 (العدد 1)، الجزائر: جامعة الشهيد حمة لخضر، الوادي، الجزائر ص.ص 303-319.

SCAN ME